

(10) International Publication Number
WO 01/11586 A1

- Published:**
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

- _____ • HARD WIRE
- _____ • RF CONNECTION
- • TELEPHONE CONNECTION

(57) Abstract: The present invention makes use of the Internet (18) and its instant messaging capability for the continual alarm monitoring of protected premises. A central web site (20) receives instant messages from premise computers (12) at computer controlled, programmable, variable time frames based on protection levels. The protected premise computer (12) sends encrypted messages both in an alarm state and in a normal state. This continual message traffic, reinforced by variable message timing established by the central web site (20) and known only to the central web site (20) and the premise computer (12), provides maximum protection against compromise of the system since the absence of a normal message or the non-appearance of an expected message will constitute an alarm. The central web site (20) dispenses alarm notification to local responders (police, fire dept., local monitors) (24) in accordance with a priority system where the most serious alarm is reported first as well as notifying the premise owners (41) via paging or other communication means. The central web site (20) communicates to the premise computer (12) to change message rates and encryption information as well as to arm the system.

WO 01/11586 A1

**TITLE: ALARM REPORTING SYSTEM USING THE
 THE INTERNET AND INSTANT MESSAGING**

5

CROSS REFERENCE TO RELATED APPLICATIONS

This application is based upon and claims the priority of US Provisional Application filed on August 5, 1999 entitled " Monitoring Residential or Commercial Premises Through the
10 Internet" whose inventor is Myles Kranzler and US Provisional Application Serial No. 60/152,535 filed on September 3, 1999 and entitled " Alarm Reporting System Using the Internet and Instant Messaging:" whose inventor is also Myles Kranzler.

BACKGROUND OF THE INVENTION

15 1. Field of Invention

This invention relates to a means to monitor many premises simultaneously using two way communications via the Internet instant messaging method and a central web site wherein each premise system will communicate periodically with the central web site based on central web site modifiable control parameters.

20

2. Description of Related Art

The majority of present systems use land line telephone or cellular phones to report alarms to a designated agency. In the normal mode of operation the premise monitoring system locally monitors the status of the alarms and only in the case of a problem seizes the phone line
25 and calls the monitoring agency for help.

This type of telephone system is known to be susceptible to easy compromise. If the phone line is cut or the cellular transmissions are disrupted, the monitoring agency will not know that an alarm is present. The majority of current systems are one way (i.e. from premise to monitoring agency). This makes modification of operation complex. Once a system is
30 programmed for a monitoring site, a change in that site would require a premise visit. This makes it difficult for the monitored premise to change monitors or have a secondary monitoring site in case of emergency at the primary monitoring site.

Current systems are able to use preprogrammed alarm sequences to assist in the determination of whether or not an alarm is false or not. These systems, however, are limited to one way communication and cannot disable or activate selected sensors to accommodate changing conditions or to establish alarm validity. U.S. 5,892,690 issued to Boatman et al
5 describes an environmental monitoring system which includes monitoring assemblies at various sites of environmental concern. Sensors measure environmental parameters, such as air quality and store the data for each site as instructed by an on-site controller. The stored data is uploaded to a central, remote database where it can be accessed and sent out to a particular site. The remote database can be connected to a distributed wide area network, e.g. the Internet. This
10 environmental monitoring system does not include means or procedures for notifying an emergency response agency when a site sensor detects a security breach. This system does not disclose means or procedures for testing the site-to-central database link for failure. The system does not require real time transmission of its data as would be required in an alarm system.

US Patent 5,400,246 issued to Wilson et al describes a peripheral data acquisition,
15 monitor and adaptive control system using a personal computer to allow the user to create a control configuration, test and change and operate the control configuration for diverse applications such as security systems. Measurement and configuration data are entered directly into the computer. Wilson et al discloses such a system adapted as a radio frequency security system for an automobile dealer in which security sensor transmitters are placed in each vehicle
20 and send signals to a central station. The transmissions are logged on the personal computer which takes appropriate action in response, such as, dialing telephones and playing recorded messages to police. Thus the Wilson et al patent also does not suggest an Internet accessible central database to be polled at the convenience of the security agency in accordance with the present invention.

25 US Patent No.4,741,022 issued to Chebra, et al describes a remote subscriber interaction system. A central control unit (scanner) is connected across a set of subscriber loops. At each subscriber's premises, an individual subscriber terminal (STU) is connected across that particular subscriber's loop. To each STU are connected the various instrumentalities which are to be monitored by the system, e.g. burglar alarms, fire alarms, etc. FSK modulated signals in the upper
30 part of the audible range are transmitted from the scanner to the STUs at appropriate times. The STU's reply by means of similar signals to indicate the status (e.g. alarm, or non-alarm) of the

instrumentalities at the respective subscriber's premises. This transmission and retransmission is interrupted when the subscriber's telephone is off hook. In addition, a signal below the audible range (low tone) is produced at the STU, and transmitted to the scanner over the telephone loop when all the instrumentalities at the particular subscriber's premises are in a given state (e.g. no
5 alarm). When the state of one instrumentality changes, low tone is stopped. Such stoppage is sensed by the scanner, and causes immediate transmission of FSK signals from the scanner to the corresponding STU, even though the associated telephone is off hook at the time. The reply to such transmission provides information about the reason for the stoppage, i.e. what is the source of the alarm.

10 The Chebra et al system can be compromised by the insertion of a bogus low tone external to the premise and a simulated off-hook condition. The system is dependant on the cooperation of the telephone company and the placement of equipment in the telephone company central office and its volume is limited by the bandwidth of the telephone system. The signals are not encrypted and because they are transmitted at a regular rate can be simulated. When low tone
15 is absent, the interrogation signal sent to the premise during the off-hook condition creates an undesirable disturbance to the user of the telephone.

US Patent No.5,861,804 issued to Fansa et al describes a security and surveillance system controlled by a computer wherein sensors monitor for certain alarm conditions which cause signals to be sent to non-data pins of a serial port of a personal computer. The personal
20 computer produces programmed responses to the alarm conditions. This disclosure relies upon the personal computer and proprietary software to alert security response agencies, for example, by cellular telephone and paging methods. Thus it lacks the central database and polling by remote security response agencies of the database via the Internet that is part of the present invention.

25 US Patent No.4,477,800 issued to O'Brien, US Patent No.4,647,914 issued to Alexander, US Patent No. 5,136,281 issued to Bonaquist and US Patent No. 5,717,379 issued to Peters are of possible relevance as representative of the general state of the art.

The aforementioned inventions fail to suggest a means or procedure for using the instant messaging feature of the Internet, afford protection against compromise through an
30 Internet accessible central database which can be programmed to poll periodically or randomly or on the occasion of a predefined event, encrypt the alarm status using a public key system, or

report alarms in accordance with a priority system where the most serious alarm gets reported first.

SUMMARY OF THE INVENTION

Briefly described, the invention comprises a premise computer, a means of
5 connecting to the Internet such as a cable modem, a wide band telephone connection or a satellite connection, a central web site with computer capability, and the instant messaging capability of the Internet.

The present invention provides a high reliability, large-scale, alarm monitoring capability using the instant messaging feature of the world wide computer network known as the Internet,
10 both to prevent compromise and to avoid the delays in alarm transmission inherent in telephone related systems. The use of the Internet provides two way communication for the purpose of modifying premise configurations through computer control at a central web site, a feature unavailable in typical telephone systems. This capability also allows the central web site to analyze and route alarm information to locally associated response sites in a priority system
15 where the most serious alarm is reported first (a feature not available in normal telephone operated systems).

The continual communication at a defined periodicity rate known only to the premise computer and the computer at the central web site insures that any attempt to compromise the system would itself cause an alarm (premise non-responding). This rate can be modified by
20 random messages sent by the central web site computer to prevent any outside determination of inter-message access.

The use of computers in both premise and Central Web Site permits encryption of alarm data and alterations with the keys under supervisory control.

The invention may be more fully understood by reference to the following drawings.
25

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow diagram that illustrates the process of gathering sensor information and the transmission of that information using the Internet instant messaging system according to the preferred embodiment of the invention.

30 FIG. 2 illustrates a sequence of events that occur when either an alarm is detected or an "I am OK" message periodic time has expired and shows a sequence of events if no message is

received when expected.

FIG. 3 illustrates a manner in which the Central Web Site determines that the premise requires a modification to its programmed actions.

5

DETAILED DESCRIPTION OF THE INVENTION

During the course of this description like numbers will be used to identify like elements according to the different views which illustrate the invention. The embodiment described in Fig 1-3 is the preferred embodiment of the system and method of performing the premise monitoring.

FIG 1 illustrates a system 100 for gathering the sensor data and transmitting to and receiving information from the central web site. The central web site 20 instantly recognizes and processes incoming messages through its continuous connection to the Internet 18. The central web site 20 uses the Internet 18 to transmit messages back to the designated premise containing the sensors 10 through an Internet Service Provider ("ISP") 16. The ISP 16 is connected to one of three known possible premise communication devices, either a cable modem 13, a wireless device operating through a satellite 15, or a wide bandwidth communication system such as a DSL 14, any one of which permits continuous connection to the Internet. The premise communication devices 13, 14 or 15 are connected to an in-premise computer 12 containing logic control. This in-premise computer 12 receives local sensor data 10 and processes this data in accordance with programmed instructions contained within its logic section.

In accordance with the invention, the premise computer 12 and central web site are initialized on installation with default monitoring information including designation of the sensors 10 connection points and communication protocol (See Fig.2 21) The premise computer 12 acquires the data and decides whether the information constitutes one or more alarm states. If it determines that an alarm is present, it will format (see description of **FIG 2**) and initiate the instant message.

If the premise computer 12 is unable to communicate using the cable modem or other communication system (13, 14 or 15) it can, alternatively, call the central web site on the telephone. The central web site 20 can download the telephone number if it changes. This information download receives an acknowledgement from the premise computer.

If no alarm state is found, the in-premise computer 12 determines if a periodic "I am OK" message is to be sent and, if so, it determines if this message is to include raw sensor data.

It then formats the message and initiates the instant message. The decision to send the message containing the raw sensor data is determined by a programmable occurrence counter.

If an alarm state is detected the central web site 20 conveys this information to the selected response provider 24 through the ISP 22 serving the response provider. The central web site 20 receives messages from many in-premise computers and informs the response provider 24 against a priority list where the most serious alarm receives top priority and is reported first (e.g. Should a panic alarm indicate an intruder, such an alarm will receive priority over a report of an open window etc.)

The premise computer 12 receives instant messages from the central web site 20 and updates its control data accordingly. If it receives a "please send last message not received" message from the central web site 20 it re-formats the previous message and re-sends it.

The premise computer 12 can either be a separate device or can operate as a background task on an existing computer.

Referring to Fig. 2, the sequence of events and the central web site 20 processing is described. The premise computer and central web site are initialized on installation with designation of sensor points and communication protocol. The in-premise computer 12 acquires data from all the sensors on a continual basis transmitting such messages to the central web site in a modifiable sequence known only to the premise computer and the central web site and, when the transmission time occurs sends an "I am OK" message or if a sensor changes state, will format 24 the sensor data into a defined packet. The packet is then encrypted 26 using a public key encryption procedure. The private and public keys will be updated at a controller programmed time period by the central web site 20. The premise computer 12 will have received the assigned central web site 20 public key at a previous time. It includes the central web site 20 public key with each message to permit the central web site 20 to verify the key that was sent. If the in-premise computer 12 loses the key it includes a blank central web site 20 public key to indicate this fact. The encrypted message is sent 28, using either the cable modem, wireless device operating through a satellite or other wide bandwidth device continually connected to the world wide computer network as an instant message with the central web site 20 (whose address has been programmed into the in-premise computer 12) as the routing recipient.

The central web site 20 receives the message 30 and using the public key supplied with the message and its own private key, deciphers the incoming message. The central web site 20

verifies that the message 30 arrived at the expected time and resets the expected time to establish when the next message should occur in accordance with a modifiable sequence. If the message contains sensor change information, the central web site 20 recognizes the status of all sensors and determines 32 if the change in sensor(s) constitutes an alarm or an expected change (e.g. store opening in the morning at 8 am is expected) and if the alarm is true or false based on a predetermined set of scenarios for each premise computer. If a alarm is determined 32, the central web site 20 determines the designated respondent 24 to that specific sensor 10 and , if a true alarm is determined, forwards the alarm information 36 in accordance with a priority system via the Internet using instant messaging or using telephone numbers previously programmed into the central web site to said respondent 24. Additionally, if requested, the premise owner is notified 41 by the central web site .The premise computer 12 continues to send the sensor change message at a 'change in sensor designated time frame' until the central web site 20 acknowledges 40 the sensor change message. This acknowledgement is not sent until the local respondent 24 acknowledges the receipt of the alarm message. Once the central web site 20 receives the local respondent's 24 acknowledgement 38, it sends the premise computer 12 an acknowledgement 40. The in-premise computer 12 reverts to the standard message time frame. Any change in local sensors recognized by the premise computer 12 are latched (i.e. kept in the changed state internally in the premise computer 12) until acknowledged by the central web site 20. Once acknowledged, the premise computer 12 interrogates the sensors active state and, if it has changed back to its original state, the premise computer 12 again reports a change of state. This insures that even a momentary change of sensor state is reported.

If the message contains updated sensor information (not a change) the Central Web Site 20 verifies 30 that that information is consistent with the present stored sensor information. If present stored sensor information is not consistent with the message as received, the central web site 20 responds by initiating a request (see Fig.3, 46) for additional information including requesting a special response code stored in the premise computer 12. If this requested information is not returned within a designated period of time or is returned with incorrect data, the Central Web Site 10 notifies (See Fig. 3, 48) a designated local respondent 24 and, if required, the premise owner 41.

Every time a message 30 is received from a specific premise computer 12, of which there is one for every subscriber, the central web site 20 updates the expected time of the next message

30. The central web site 20 has a queue of expected messages and their times. If a message is not received within the expected time (plus a defined tolerance), the central web site 20 initiates and alarm state and immediately notifies 34 the associated respondent 24 and the premise owner 41

5 . If the central web site 20 determines that all or part of the means for Internet transmission is disabled, it reverts to monitoring a telephone input for alarm information. If the premise computer 12 does not receive an acknowledgement of its change of sensor message or recognizes that the means for Internet access is down and has a change of sensor, it uses a backup telephone or cell phone to communicate with Central Web Site 20. This communication method is self limited to reporting only on change of state in order not to overload the telephone system.

10 Referring to Fig. 3, the central web site 20 can issue requests for sensor data transmission or the retransmission of non-received data to determine loss of communication or verification of premise status. If 46 present stored information is not consistent with a message as received, the central web site 20 initiates a request for additional information including special response code stored in the premise computer. The central web site 20 formats and encrypts 48 the
15 message and transmits to the premise computer 12 using its instant messaging capability. The premise computer 12 decrypts the message and responds 50 to the central web site 20. If the requested information is not returned 52 within designated period or is returned with incorrect data, the central web site 20 notifies the designated local respondent 24. Additionally, the central web site 20 notifies the premise computer 12 of changes to reporting schedules or central web
20 site 20 Internet address or backup dial out telephone numbers. Once the transmission request is formatted for transfer to the premise, 53 the central web site 20 sends the message to the premise computer 12.

The premise computer 12 receives the message 54 and either updates its internal control parameters and / or responds with the requested information.

25 In summary, the invention provides protection against compromise by transmitting "I am alive" encrypted messages to a central web site monitoring the premise in accordance with a modifiable program known only to that central web site and the monitored premise thereby avoiding bogus "I am alive" messages. The invention makes use of the instant messaging system available only through the Internet to eliminate the delays inherent in standard telephone
30 communication providing the added protection of timely responses to emergencies. The use of the instant messaging system and the two way communication permits the assessment of real or

false alarms in real time and offers the opportunity to eliminate unnecessary police, fire, or medical response.

While the invention herein disclosed has been described by specific embodiments and applications thereof, it is understood that numerous modifications and variations can be made
5 thereto by those of ordinary skill in the art without departing from the spirit and scope of the present invention.

What is claimed is:

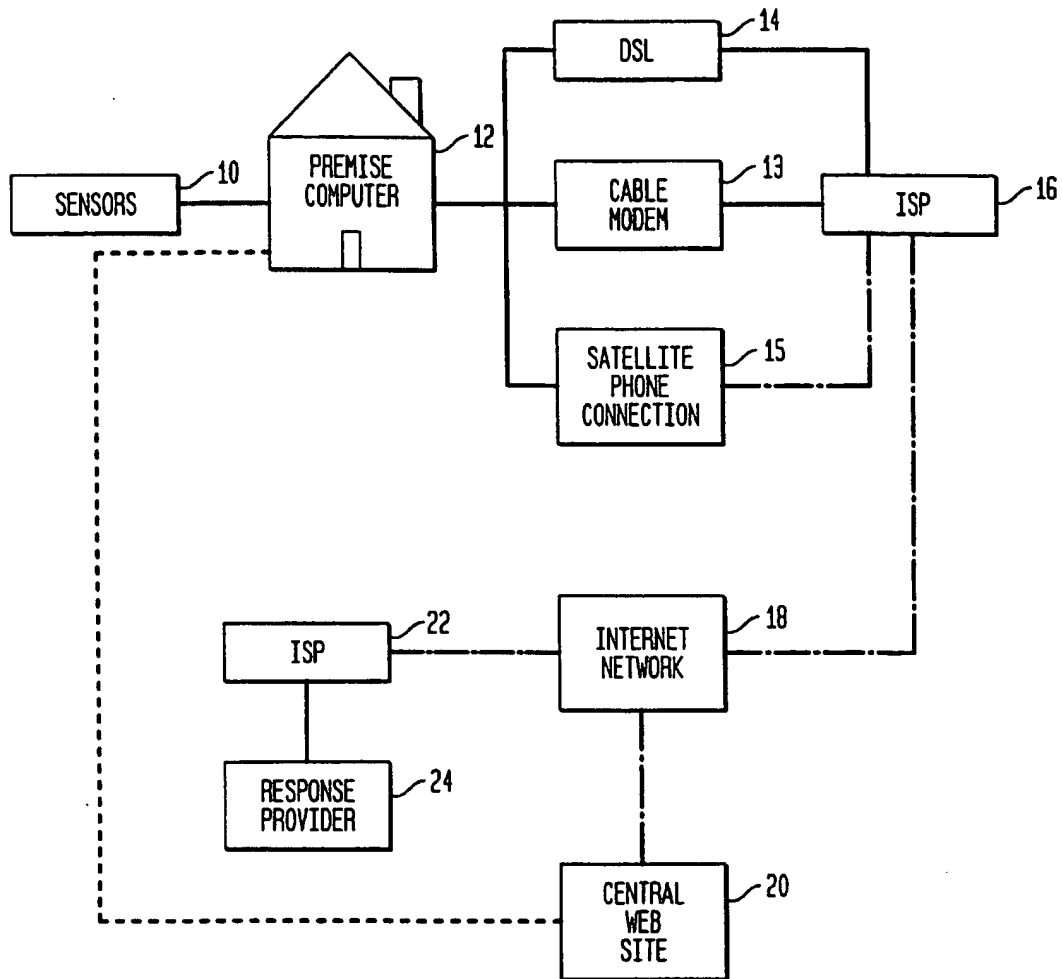
1. A system for monitoring premise alarm sensors (10) over a world wide computer network (18).
2. A system according to Claim 1 further comprising that the connection to the world wide
5 computer network (18) shall be from a premise computer (12) through a device including but not limited to a cable modem (13), a wide band telephone system (14), and a satellite connection (15) which is continually connected to the world wide computer network (18).
3. A system according to Claim 2 further comprising means to transmit data from the
10 premise computer (12) to a central web site (20) and from the central web site (20) to the premise computer (12).
4. A system according to Claim 3 further comprising means for the central web site (20) to preprogram the premise computer (12) to issue status messages in accordance with a modifiable sequence.
5. A system according to Claim 4 further comprising means for programming the premise
15 computer (12) with sensor designation and communication protocol with the central web site (20).
6. A system according to Claim 5 further comprising means for programming the central web site (20) to recognize the status of all alarm sensors (10).
7. A system according to Claim 6 wherein the premise computer (12) issues alarm status
20 messages in a modifiable preprogrammed sequence for recognition by the central web site (20) in a matching sequence known only to the premise computer (12) and the central web site (20) such that omission or corruption of the status message represents an alarm condition.
8. A system according to Claim 7 further comprising means where a change in the status of
25 an alarm message initiates a message to the central web site (20).
9. A system according to Claim 8 further comprising a central web site (20) for updating the local premise computer (12) control information.
10. A system according to Claim 9 wherein the data from the premise computer (12) and the central web site (20) is encrypted using a public key methodology.
- 30 11. A system according to Claim 10 wherein the status messages can be requested on command from the central web site (20).

12. A system according to Claim 11 further comprising means to use the instant messaging feature of the world wide computer network (18) for requesting immediate reporting of information.
13. A system according to Claim 12 wherein the alarm status is reported to selected response providers (24) and a premise owner (41) in accordance with a priority system where the alarm determined to be the most serious is reported first.
14. A method for monitoring premise alarm sensors (10) using the world wide computer network (18) and two way instant messages wherein said method comprises the following steps irrespective of sequence:
- a) programming the premise computer (12) with sensor (10) designation and communication protocol and initiating continual communication with a central web site (20);
 - b) programming the central web site (20) to recognize the status of all alarm sensors (10);
 - c) transmitting periodic status messages from the premise computer (12) in accordance with a preprogrammed schedule generated at the central web site (20);
 - d) indicating a change in the status of an alarm sensor (10) and sending an instant message to the central web site (20) at the time of occurrence;
 - e) interpreting messages received at the central web site (20) and indicating an alarm status; and,
 - f) communicating an alarm status to a service provider (24) such as fire, police, or medical facilities in accordance with a priority system.
15. A method according to Claim 14 further comprising the following steps irrespective of sequence:
- g) continuously communicating between the premise computer(12) and the central web site (20) using either a cable modem (13), wide band telephone connection (14) or satellite connection (15);
 - h) activating a public key and a private key in the premise computer (12) and a different public key and private key in the central web site (20)

- i) formatting the status of the alarm sensors (10) as a digital message and encrypting the message;
- j) transmitting the encrypted message to the central web site (20);
- k) decrypting the message at the central web site (20) using its private key;
- l) acting upon the message at the central web site (20) in accordance with predefined rules;
- m) communicating instructions and commands from the central web site (20) to the premise computer (12) using the premise public key; and,
- n) decrypting these commands at the premise computer (12) using its private key.
16. A method according to Claim 14 further comprising the following steps:
- o) programming a random code generator at the central web site (20) to periodically establish a timing schedule for premise computer (12) reporting purposes;
- p) encrypting and transmitting the schedule to the premise computer (12); and,
- q) decrypting the message by the premise computer (12) and adjusting the premise computer (12) clock system to transmit status messages in accordance with the new program.
17. A method according to claim 14 wherein the sequence of alarms reported by the premise computer (12) is used to discriminate between true and false alarms said method comprising the steps of:
- r) programming the central web site (20) with the type and location of sensors (10) in the premise; and,
- s) transmitting changes from the premise computer (12) as to the status of the alarm sensors (10) and analyzing the changes at the central web site (20) in the status of the alarm sensors (10) against a predetermined set of scenarios to discriminate between true and false alarms.

18. A method according to claim 14 wherein the central web site (20) can update the premise computer (12) control information and said method further comprising the following steps:
- t) entering commands into the central web site (20) to change information to the premise computer (20);
 - u) transmitting said commands from the central web site (20) as priority messages to the premise computer (12);
 - v) receive and acknowledge the new information at the premise computer (12) and adjust the premise computer's (12) internal control programs to comply with said command.
19. A method according to claim 14, wherein the premise computer (12) will periodically transmit either sensor status or an "I am OK" message using this communication to establish the alarm situation.
20. A method according to claim 14 wherein the reception of a periodic message will itself be considered a no-alarm condition.
21. A method according to claim 14 wherein a central web site (20) can update the local premise computer (12) control information and request immediate reporting of information by using the world wide computer network (18) and instant messages.
22. A method according to claim 14 wherein the central web site (20) transmits alarm data to selected response agencies (24) and the owner (41) using the instant messaging system of the world wide computer system (18) said method further comprising the following steps irrespective of sequence:
- w) programming the central web site (20) with the telephone addresses of selected response agencies (24) and the telephone number of the premise owner (41);
 - x) programming the central web site (20) to report alarms to selected agencies (24) upon receipt of such alarms from premise computers (12);
 - y) receive from the central web site (20) the status changes indicating an alarm situation; and,
 - z) connect the central web site (20) to the appropriate agency (24) and report the alarm and telephone the premise owner (41) and report the alarm.

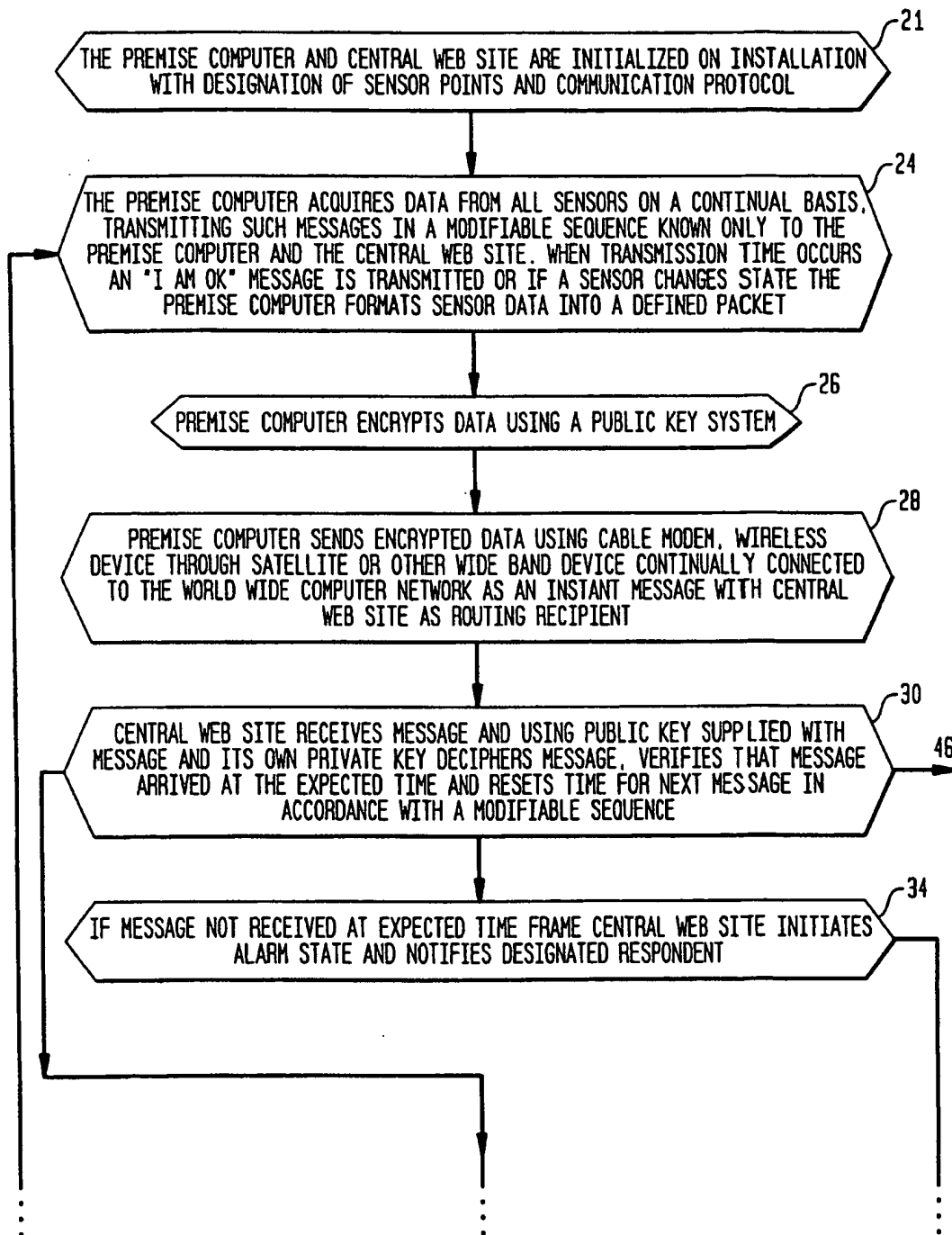
FIG. 1



— = HARD WIRE
— = RF CONNECTION
--- = TELEPHONE CONNECTION

2/4

FIG. 2A



3/4

FIG. 2B

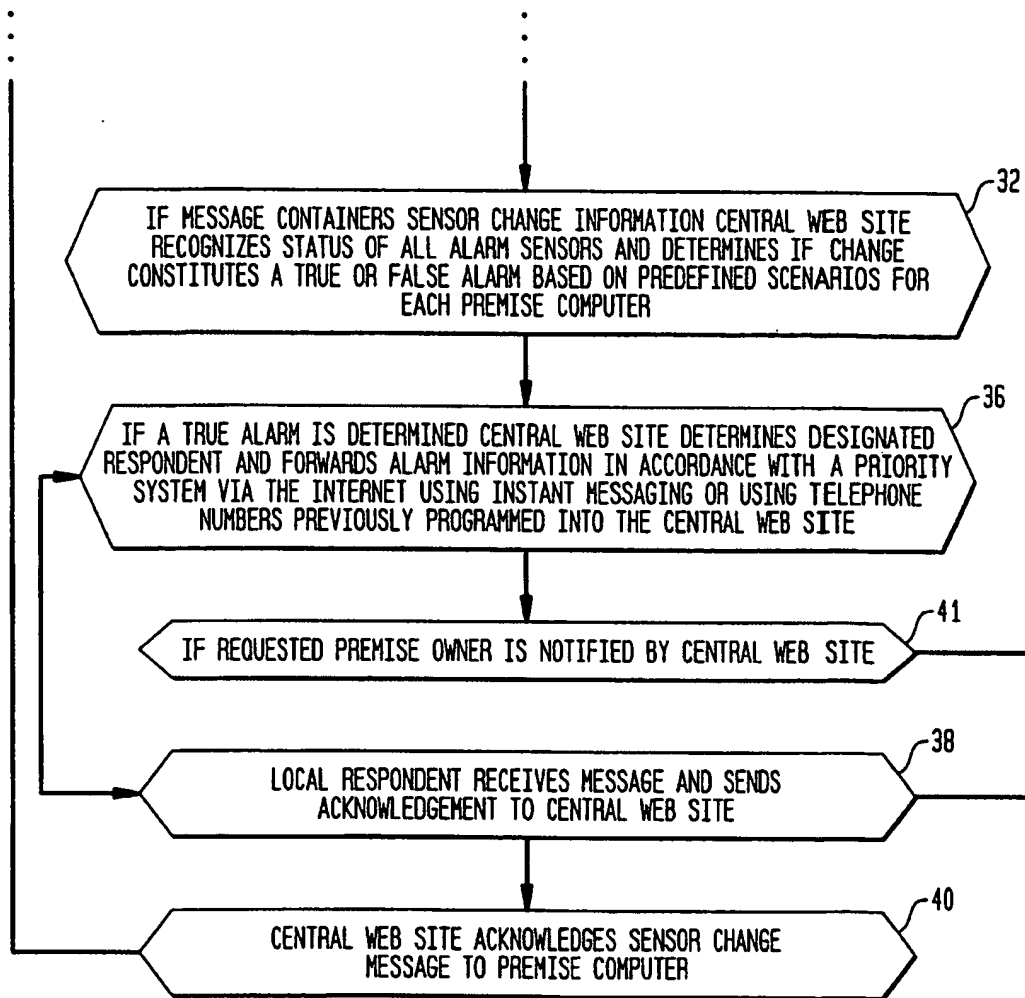
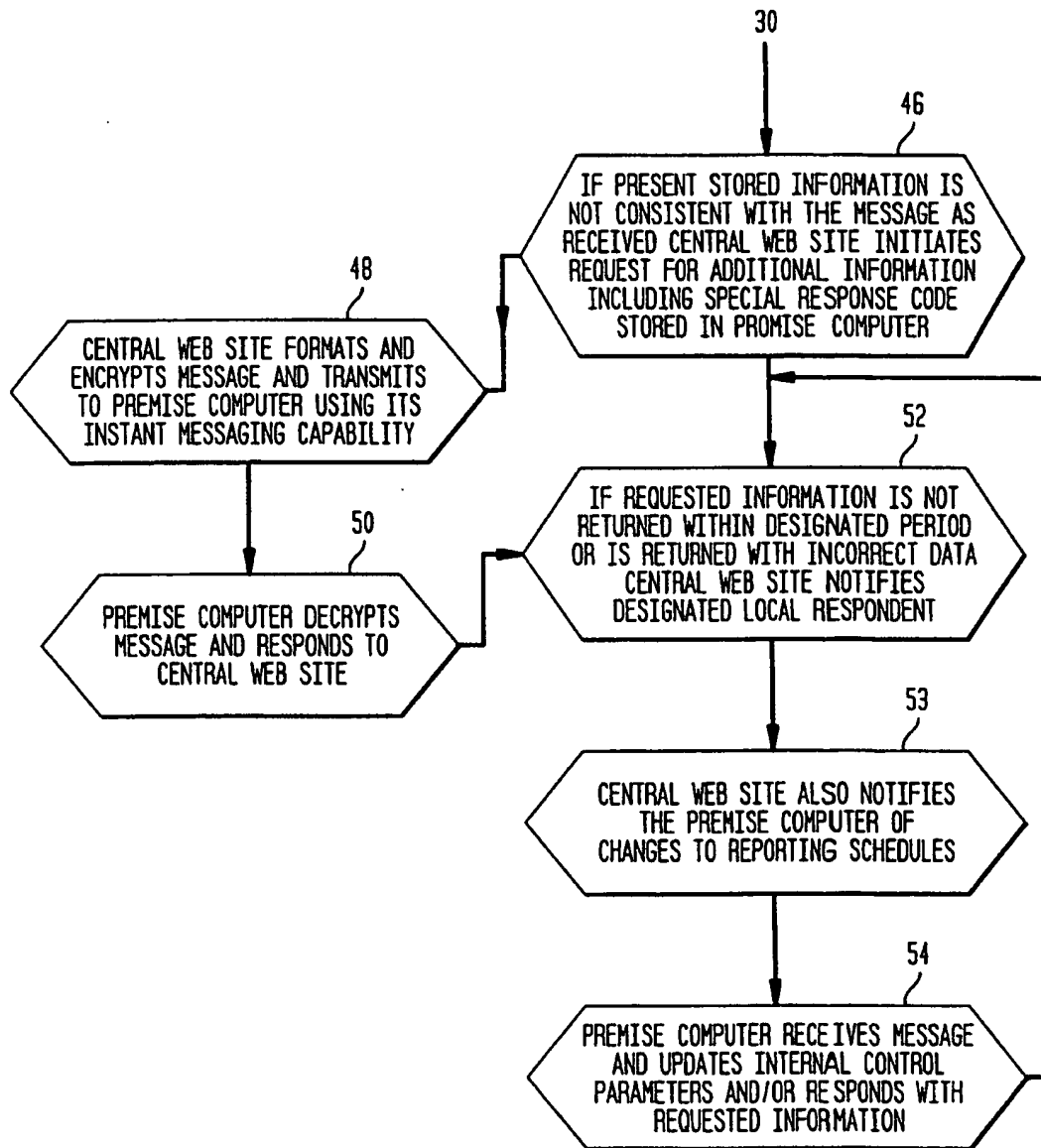


FIG. 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/07775

A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : G08B 29/00 US CL : 340/506 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 340/506, 825.06, 521, 539, 531, 825.69; 379/37, 38; 370/913 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) BRS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 6,060,994 A (CHEN) 09 May 2000, col. 2, lines 35-50	1-9
Y,E		10-17
Y,P	US 5,974,141 A (SAITO) 26 October 1999, Abstract	10-13 and 15-17
Y	US 5,892,690 A (BOATMAN et al) 06 April 1999, col. 1, lines 45-58	14-17
A	US 5,638,448 A (NGUYEN) 10 June 1997, ALL	1-17
A	US 5,917,405 A (JOAO) 29 June 1999, ALL	1-17
A,P	US 6,023,223 A (BAXTER, JR) 08 February 2000, ALL	1-17
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family		
Date of the actual completion of the international search 30 JUNE 2000		Date of mailing of the international search report 31 JUL 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer JOHN TWEEL, JR. <i>Rugenia Zogan</i> Telephone No. (703) 308-7826